Mobile messaging apps in humanitarian emergencies

Prepared by:
Lina Jasmontaite
September 29, 2017
Rennes
Outline

• Handbook on Data Protection in Humanitarian Action
• The use of smartphones by refugees and migrants
• The use of mobile messaging apps by humanitarian organizations
  • Communication tools
  • Purposes
• Risks associated with the use mobile messaging apps
  • Types of collected data
  • Remaining challenges
Handbook on Data Protection in Humanitarian Action

ACADEMIC PRIVACY RES
CENTRE IN THE HEART OF
EUROPE

News
22 September 2017 • Hub Co-Director
Christopher Kuper speaks at EU workshop on
ePrivacy
4 September 2017 • Delegation from Chuo
University in Tokyo visits the Hub

Events
SEPTEMBER
29
Les données numériques des
migrants et des réfugiés

OCTOBER
5
GDPR Workshop Series: The
Implications of the GDPR for
Research Involving Genetic Data

Handbook on Data Protection in Humanitarian Action

This Handbook was published as part of the Brussels Privacy Hub
and ICRC’s Data Protection in Humanitarian Action project. It is
aimed at the staff of humanitarian organizations involved in
processing personal data as part of humanitarian operations,
particularly those in charge of advising on and applying data
protection standards.

The Handbook builds on existing guidelines, working procedures
and practices established in humanitarian action in the most
volatile environments and for the benefit of the most vulnerable
victims of humanitarian emergencies. It seeks to help
humanitarian organizations comply with personal data protection
standards, by raising awareness and providing specific guidance
on the interpretation of data protection principles in the context of
humanitarian action, particularly when new technologies are
employed.
The use of smartphones by refugees and migrants
The use of mobile messaging apps by humanitarian organizations

Multiple communication channels
The use of mobile messaging apps by humanitarian organizations

Purposes:
• to **target audiences** (staff or beneficiaries) already using messaging apps;
• to **reduce** communications **costs**;
• to **maintain reliable contact** with people (whether staff or beneficiaries) in transit;
• to enable communication with people in environments where other communications methods are unavailable;
• to increase the speed of communications;
• to **improve the security** of digital communications as compared with existing methods of communication;
• to **facilitate** information **collection** from or **dissemination** to hard-to-reach, remote or inaccessible areas;
• to **speed up data collection** or increase efficiency; and
• to improve inter-office coordination.
## Risks associated with the use of mobile messaging apps

### Types of collected data:
- Message content
- User information
- Metadata
- Data shared with third party providers
- Evidence that a user has installed an app on their phone

### Ways for third parties to access data shared over messaging apps:
- A disclosure request from an authority to a messaging app company
- Unlawful or covert access to message content or metadata stored on a messaging app company’s servers
- Parties access messaging app content through other covert methods
- An individual is forced to hand over their physical device
- A messaging app company allows an authority to direct access to content or data transmitted by building a ‘secret feature’
Challenges associated with the use of mobile messaging apps

1. Selection of appropriate communication tools

2. Implementation of general data protection principles, such as
   a) Notification;
   b) Purpose limitation;
   c) Rights to rectification and deletion;
   d) Data minimization; and
   e) Limited data retention

3. Acceptance of additional obligations
Thank you!

lina.jasmonitaite@vub.ac.be